



# UNITED STATES PATENT AND TRADEMARK OFFICE

THW  
UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/645,989	08/22/2003	William E. Sobel	20423-08016	8643
45969	7590	03/07/2006	EXAMINER	
SONNENSCHEIN NATH & ROSENTHAL LLP FOR SYMANTEC CORPORATION P. O. BOX 061080 WACKER DRIVE STATION, SEARS TOWER CHICAGO, IL 60606-1080			KIM, PAUL	
		ART UNIT		PAPER NUMBER
		2161		
DATE MAILED: 03/07/2006				

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/645,989	SOBEL, WILLIAM E.
	Examiner	Art Unit
	Paul Kim	2161

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 22 August 2003.  
 2a) This action is FINAL.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-27 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-27 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 22 August 2003 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

  
**SAM RIMELL**  
**PRIMARY EXAMINER**

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
 Paper No(s)/Mail Date 2.
- 4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application (PTO-152)  
 6) Other: \_\_\_\_\_.

**DETAILED ACTION**

1. This Office Action is responsive to the following: Original Application filed on August 22, 2003.
2. Claims 1-27 are pending. Claims 1, 9, and 16 are independent.

***Drawings***

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description:

- Figure 5, element 515.

Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either “Replacement Sheet” or “New Sheet” pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

***Claim Rejections - 35 USC § 112***

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claims 1- 27** are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

6. **As per independent claim 1**, the claim recites “attributes” in lines 10 and 17. It is unclear whether applicant intends this recitation to be the same as or different from “file attributes” recited in line 2 of the claim.

7. **As per dependent claims 2-3**, the claim recites “a specific file” in lines 2-3. It is unclear whether applicant intends this recitation to be the same as or different from “a specific file” recited in line 19 of claim 1.

8. **As per dependent claim 4**, the claim recites “attributes” in line 2. It is unclear whether applicant intends this recitation to be the same as or different from “file attributes” recited in line 2 of claim 1.

a. Additionally, the claim recites “a record in the database” in line 3. It is unclear whether applicant intends this to be the same as or different from “a record in the database” in line 18 of claim 1.

b. Additionally, the claim recites “a specific file” in line 4. It is unclear whether applicant intends this to be the same as or different from “a specific file” in line 19 of claim 1.

9. **As per claims 5-27**, the claims contain similar types of deficiencies as those described with respect to claims 1-4, the number a nature of which is too numerous to mention each individually. It is incumbent upon Applicant to ensure any amendment addresses the deficiencies of claims 5-27 in addition to those specifically noted with respect to claims 1-4.

*Claim Rejections - 35 USC § 101*

10. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

11. **Claims 9-15** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 9-15 recite “a computer readable medium contain a computer program product . . . comprising program code” which is software, *per se*, and therefore is non-statutory subject matter.

*Claim Rejections - 35 USC § 102*

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

13. **Claims 1-3, 6, 8-11, 14, 16-18, and 21** are rejected under 35 U.S.C. 102(b) as being anticipated by Pisello et al (U.S. Patent No. 5,495,607, hereinafter referred to PISELLO), filed on November 15, 1993, and issued on February 27, 1996.

14. **As per independent claim 1, 9 and 16, PISELLO teaches:**

A computer implemented method for gleaning file attributes independently of file format, the method comprising the steps of:

A non-application specific file attribute manager receiving a plurality of files in a plurality of formats {See PISELLO, col. 13, lines 14-19, wherein this reads over “a domain-wide status-monitor . . . periodically scan[s]”};

The file attribute manager scanning the plurality of received files in the plurality of formats {See PISELLO, col. 13, lines 14-19, wherein this reads over “a domain-wide status-monitor . . . periodically scan[s]”};

The file attribute manager gleaned attributes concerning each of the plurality of scanned files in the plurality of formats {See PISELLO, col. 13, lines 48-51, wherein this reads over “to collect the file identifying information stored at a given scan time”; and col. 15, lines 36-51, wherein this reads over, searchable database fields preferably include: . . . FileName;PathName”};

The file attribute manager storing gleaned attributes concerning each of the plurality of scanned files as records in a database {See PISELLO, col. 13, lines 51-56, wherein this reads over “to integrate the collected information into the domain-wide virtual catalog”}; and

The file attribute manager indexing attributes being stored as a record in the database concerning a specific file according to contents of that file {See PISELLO, col. 14, lines 16-19, wherein this reads over “Table 2 which shows an example of what might be displayed . . . [from] the domain administrating data/rule base”}.

15. **As per dependent claims 2, 10, and 17, PISELLO teaches:**

A method wherein the specific gleaned attributes concerning a specific file are a function of a protocol according to which the file is transmitted {See PISELLO, Table 2, wherein this includes the file-server name under the column labeled “File\_Source” and the sender name under the column labeled “By”}.

16. **As per dependent claim 3, 11, 18, PISELLO teaches:**

A method wherein the specific gleaned attributes concerning a specific file are a function of the format of that file {See PISELLO, col. 15, lines 46-51, wherein this reads over “Novell-defined attributes”}.

17. **As per dependent claims 6, 14, 21, PISELLO teaches:**

A method further comprising the file attribute manager receiving a plurality of copies of the same file, and the file attribute manager storing a separate record for each received copy of the file, each record being indexed according to the contents of the file, such that each record can be accessed by the single index {See PISELLO, Table 2; and col. 14, lines 62-64, wherein this reads over “the same file name may appear multiple times in the listing of Table 2, even with identical path names (e.g., ‘Dave.doc’)”}.

18. **As per dependent claim 8, PISELLO teaches:**

The method wherein the non-application specific file attribute manager is incorporated into a server or a client {See PISELLO, col. 13, lines 14-15, wherein this reads over “domain-wide status-monitor and control program is installed in the domain administrating server”}.

*Claim Rejections - 35 USC § 103*

19. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

20. **Claims 4, 12, and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over PISELLO, in view of Fischer (U.S. Patent No. 5,694, 569, hereinafter referred to as FISCHER), filed on June 5, 1995, and issued on December 2, 1997.

PISELLO teaches the limitations of claims 1-3, 6, 8-11, 14, 16-18, and 21 for the reasons stated above.

PISELLO differs from the claimed invention in that PISELLO fails to disclose a method further comprising the file attribute manager indexing attributes being stored by using a secure hash of the contents of that file (claims 4, 12, and 19).

21. **As per dependent claim 4, 12, and 19,** PISELLO, in combination with XXXX, discloses a method further comprising the file attribute manager indexing attributes being stored as a record in the database concerning a specific file according to a secure hash of the contents of that file {See FISCHER, col. 1, lines 40-50, wherein this reads over “file integrity may be protected by taking a one-way hash over the contents of the file. By implementing and checking a currently computed hash value, with a previously stored hash value”}.

The combination of inventions disclosed in PISELLO and FISCHER would disclose a method wherein the file attribute manager would index attributes in a database according to a secure hash, by using a secure has algorithm (SHA), of the contents of that file. Therefore, it would have been obvious to one of ordinary skill in the art at the time

the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by FISCHER.

One of ordinary skill in the art would have been motivated to do this modification so that the records may be indexed securely and subsequently retrieved by a blocking system.

22. **Claims 5, 13, and 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over PISELLO, in view of Baker (USPGPUB No. 2003/0233352, hereinafter referred to as BAKER), filed on March 19, 2003, claiming priority to March 21, 2002, and published on December 18, 2003.

PISELLO teaches the limitations of claims 1-3, 6, 8-11, 14, 16-18, and 21 for the reasons stated above.

PISELLO differs from the claimed invention in that PISELLO fails to disclose a method further comprising the file attribute manager indexing attributes according to a cyclical redundancy check of the contents of that file (claims 5, 13, and 20).

23. **As per dependent claims 5, 13, and 20,** PISELLO, in combination with BAKER, discloses a method further comprising the file attribute manager indexing attributes being stored as a record in the database concerning a specific file according to a cyclical redundancy check of the contents of that file {See BAKER, Para. 0008, wherein this reads over “[t]he controller may be further programmed . . . to determine a cyclical redundancy check of the file”}.

The combination of inventions disclosed in PISELLO and BAKER would disclose a method wherein the file attribute manager would index attributes in a database

according to a cyclical redundancy check of the contents of that file. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by BAKER.

One of ordinary skill in the art would have been motivated to do this modification so that the records may be indexed securely and subsequently retrieved by a blocking system.

24. **Claims 7, 15, and 22** are rejected under 35 U.S.C. 103(a) as being unpatentable over PISELLO, in view of Chino et al (USPGPUB 2002/0046207), filed on June 25, 2001, and published on April 18, 2002.

PISELLO differs from the claimed invention in that PISELLO fails to disclose a method which deletes records from the database after the records have been stored for a specific period of time (claims 7, 15, and 22).

25. **As per dependent claims 7, 15, and 22,** PISELLO, in combination with CHINO, discloses a method further comprising of deleting records from the database after the records have been stored for a specific period of time {See CHINO, Para. 0060, wherein this reads over “location information collector determines whether a predetermined time , e.g. two hours, has passed wince the record of the current location registered in the respective tables of the location information storage was collected, and sequentially deletes those records with a predetermined time elapsed”}.

The combination of inventions disclosed in PISELLO and CHINO would disclose a method comprising of deleting records with a predetermined time elapsed. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was

made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by CHINO.

One of ordinary skill in the art would have been motivated to do this modification so that the database is kept current and free of obsolete records.

26. **Claims 23-27** are rejected under 35 U.S.C. 103(a) as being unpatentable over PISELLO, in view of Touboul (U.S. Patent No. 6,092,194, hereinafter referred to as TOUBOUL), filed on November 6, 1997, and issued on July 18, 2000.

PISELLO teaches the limitations of claims 1-3, 6, 8-11, 14, 16-18, and 21 for the reasons stated above.

PISELLO differs from the claimed invention in that PISELLO fails to disclose a method for retrieving at least one stored record concerning the file, and thereafter determining a status concerning the file (claim 23).

PISELLO differs from the claimed invention in that PISELLO fails to disclose a method for blocking malicious files (claim 24).

PISELLO differs from the claimed invention in that PISELLO fails to disclose a method for allowing legitimate files (claim 25).

27. **As per dependent claim 23**, PISELLO, in combination with TOUBOUL, discloses the following:

A method further comprising:

Examining a file, the file having been processed by the non-application specific file attribute manager {See TOUBOUL, col. 7, lines 46-59, wherein this reads over “[t]he ID generator in step 604 generates a Downloadable ID identifying the received Downloadable”};

Retrieving at least one stored record concerning the file from the database {See TOUBOUL, col. 7, lines 60-64, wherein this reads over “first comparator in step

608 examines the lists of Downloadables to allow or to block per administrative override"};

Analyzing gleaned attributes concerning the file, the gleaned attributes having been retrieved from at least one record concerning the file in the database {See TOUBOUL, col. 8, lines 10-14, wherein this reads over "the URL comparator in step 616 compares the URL embodied in the incoming Downloadable against the URLs of the URL rules bases"}; and

Responsive to analyzing the gleaned attributes, determining a status concerning the file {See TOUBOUL, col. 8, line 63 – col. 9, line 19, wherein this reads over "receiving the results from the first comparator, from the ACL comparator, from the certificate comparator, and from the URL comparator" and "the policy selector in step 664 indicates that the Downloadable should not pass"}.

The combination of inventions disclosed in PISELLO and TOUBOUL would disclose a method comprising of examining a file, analyzing the gleaned attributes concerning the file with records retrieved from the database (e.g. "certificate" and "URL" details), and determining the status of the file (i.e. to allow or block the file). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by TOUBOUL.

One of ordinary skill in the art would have been motivated to do this modification so malicious or illegitimate files are blocked from entering the computer, from executing, and from performing certain functions while executing.

28. **As per dependent claim 24**, PISELLO, in combination with TOUBOUL, discloses a method of blocking a file upon the determination that the received file is malicious {See TOUBOUL, col. 9, lines 13-19, wherein this reads over "the policy selector in step 664 indicates that the Downloadable should not pass . . . [and] informs the user the user that the incoming Downloadable has been blocked"}.

The combination of inventions disclosed in PISELLO and TOUBOUL would disclose a method comprising of blocking the file (i.e. or not allowing passage) upon the determination that the received file is malicious (e.g. where the policy selector indicates whether or not a Downloadable should pass to the user). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by TOUBOUL.

One of ordinary skill in the art would have been motivated to do this modification so malicious or illegitimate files are blocked from entering the computer, from executing, and from performing certain functions while executing.

29. **As per dependent claim 25, PISELLO, in combination with TOUBOUL, discloses a method of not blocking the file upon the determination that the received file is legitimate {See TOUBOUL, col. 9, lines 1-19, wherein this reads over “the policy selector may indicate that the logical engine pass the Downloadable if it passes one of the tests”}.**

The combination of inventions disclosed in PISELLO and TOUBOUL would disclose a method comprising of allowing the file (e.g. “Downloadable”) upon the determination that the received file is legitimate (e.g. where the policy selector indicates that the Downloadable has passed a certain test). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by TOUBOUL.

One of ordinary skill in the art would have been motivated to do this modification so non-malicious or legitimate files are allowed to enter the computer, to execute, and to performing certain functions while executing.

30. **As per dependent claim 26, PISELLO, in combination with TOUBOUL,** discloses a method for applying a rule specifying how to use gleaned file attributes to process the file {See TOUBOUL, col. 8, lines 7-13, wherein this reads over “the URL comparator in step 616 compares the URL embodied in the incoming Downloadable against the URLs of the URL rule bases”}.

The combination of inventions disclosed in PISELLO and TOUBOUL would disclose a method comprising for applying a rule specifying how to use gleaned file attributes to process a file. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by TOUBOUL.

One of ordinary skill in the art would have been motivated to do this modification in order to determine the maliciousness or legitimacy of a file by analyzing and processing the gleaned attributes according to a set rule.

31. **As per dependent claim 27, PISELLO, in combination with TOUBOUL,** discloses a method for determining a rule to apply specifying how to use gleaned file attributes to process the file {See TOUBOUL, Figure 6, wherein if “URL comparison” is not required, the method proceeds to the “ACL comparison,” which if not required goes to the “TCL comparison”}.

The combination of inventions disclosed in PISELLO and TOUBOUL would disclose a method comprising of determining at least one of a plurality of rules to apply

to a file. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the above invention suggested by PISELLO by combining it with the invention disclosed by TOUBOUL.

One of ordinary skill in the art would have been motivated to do this modification so that upon the failure or passage of a file in a rule, further gleaned attributes may be checked to determine the maliciousness and legitimacy of a file.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul Kim whose telephone number is (571) 272 2737. The examiner can normally be reached on M-F, 9am - 5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Safet Metjahic can be reached on (571)272-4023. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Paul Kim  
Patent Examiner, Art Unit 2161  
Technology Center 2100



**SAM RIMELL**  
**PRIMARY EXAMINER**